

Federal Bridge CA Certificate Policy Change Proposal

Change Serial Number: 2001-10

Title: Permit suspension of certificates for Agencies

Date: 05 November 2001

Version and Date of Certificate Policy Requested to be changed:

X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), dated 14 June 2001

Change Advocate Contact Information:

Name: Mike Jenkins
Organization: DoD
Telephone number:
E-mail address: mjenki@missi.ncsc.mil

Organization requesting change: CPWG

Change summary: The CP will be changed from prohibiting suspension of certificates to allowing Agencies to suspend certificates, and place certain conditions on its use. The CP will continue to prohibit suspension for the FBCA.

Background:

Section 4.4.2 currently prohibits use of suspension for certificates. Suspension is defined as revoking a certificate, with the reason code set to 'hold'. The certificate may then be removed from the CRL at a later date, or it can be revoked for another reason code.

When a certificate is suspended, the issuing CA is asserting that the binding between name and key in the subscriber's (suspended) certificate is in question. When the question is resolved, the CA either reasserts the binding, or dissolves the binding, from the time of the suspension. That is, the CA either removes the certificate from a subsequent CRL, or changes the listing of the certificate on the CRL to another reason code, with the date of the suspension.

When validating a signature made with a key whose corresponding certificate has been suspended, the CRL that contains the suspension entry is not sufficient; a subsequent CRL that contains the resolution to the suspension must be used.

Specific Changes:

Existing text:

Section 4.4.2, Suspension:

Suspension shall not be used by the FBCA or Agency CAs.

Proposed revised text:

Suspension shall not be used by the FBCA.

Agency CAs may use suspension (revoke a certificate with the "hold" reason code). Where suspension is used, relying parties use current information for certificate validation, and do not use retroactive certificate status.

Estimated Cost:

There is no financial cost associated with implementing this change.

Implementation Date:

This change will be implemented immediately.

Prerequisites for Adoption:

There are no prerequisites.

Plan to Meet Prerequisites:

There are no prerequisites.

Approval and Coordination Dates:

Date presented to CPWG: 05 November 2001

Date CPWG recommended approval: 2001

Date Presented to FPKI PA:

Date of approval by FPKI PA: